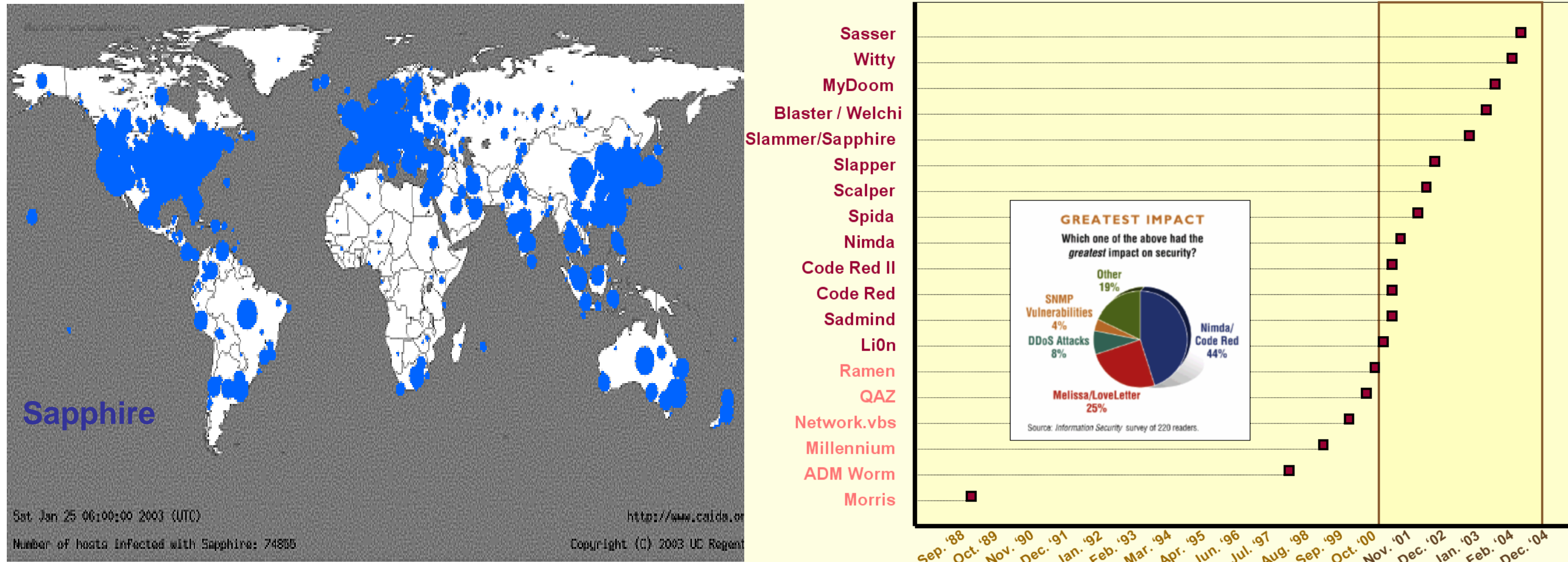


CERIAS

WormHole : A Gigabit Worm Filter using Network Processor Technology

Kihong Park (PI), Ikkyun Kim, Bhagya Betala

Problem Domain: Worm Attack



Objective : Worm Attack Protection

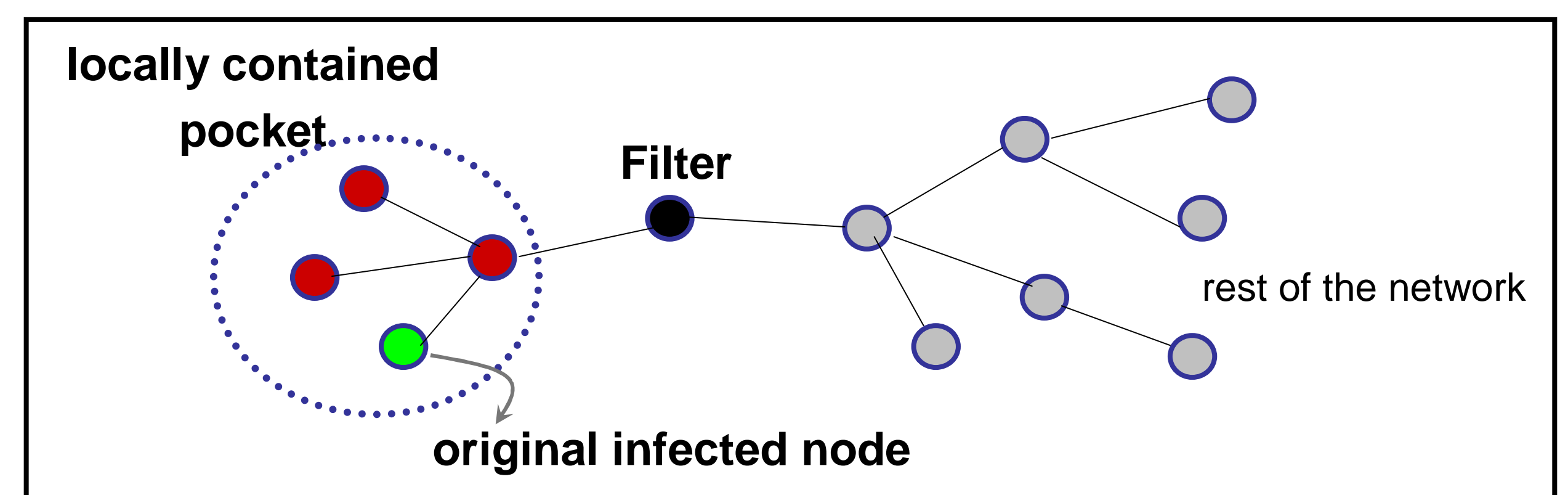
Proactive protection against known worms

→ containment: prevent spreading of infection

e.g., Blaster, Sapphire, Code Red

different from general virus filtering

Containment Pocket



Design Philosophy

Most Frequent Traffic First : *Amdahl's law*

Identifies Non-Worm Traffic for immediate pass-through

: Bloom Filter Multiple Hashing

Multi-level Caching : Differentiated Processing Speed

while allowing run-time programmability.

Highlights

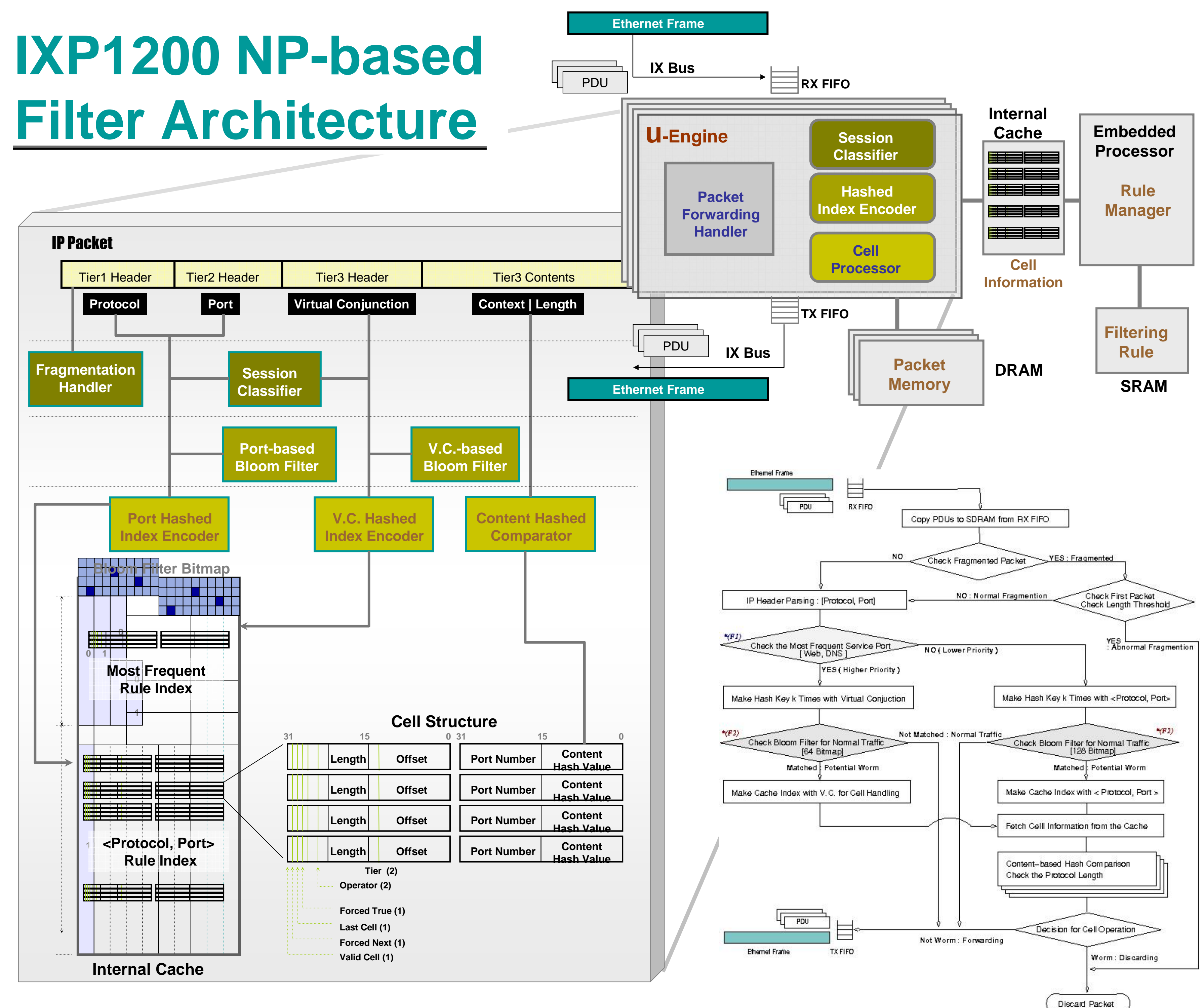
Protocol Length Check

Multiple Bloom Filter for Time & Space Complexity

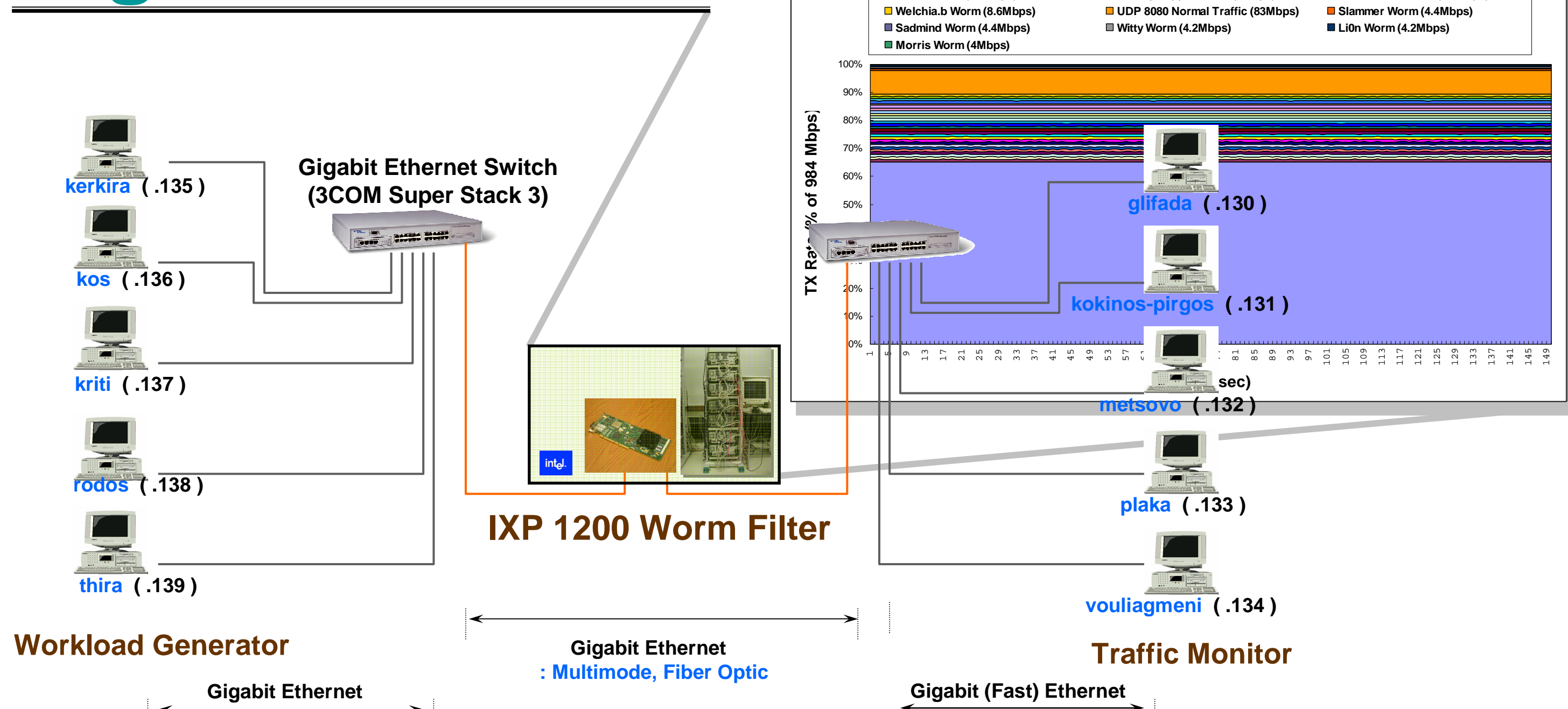
Contents-based Hash Comparison

Virtual Conjunction based Rule Optimization

IXP1200 NP-based Filter Architecture

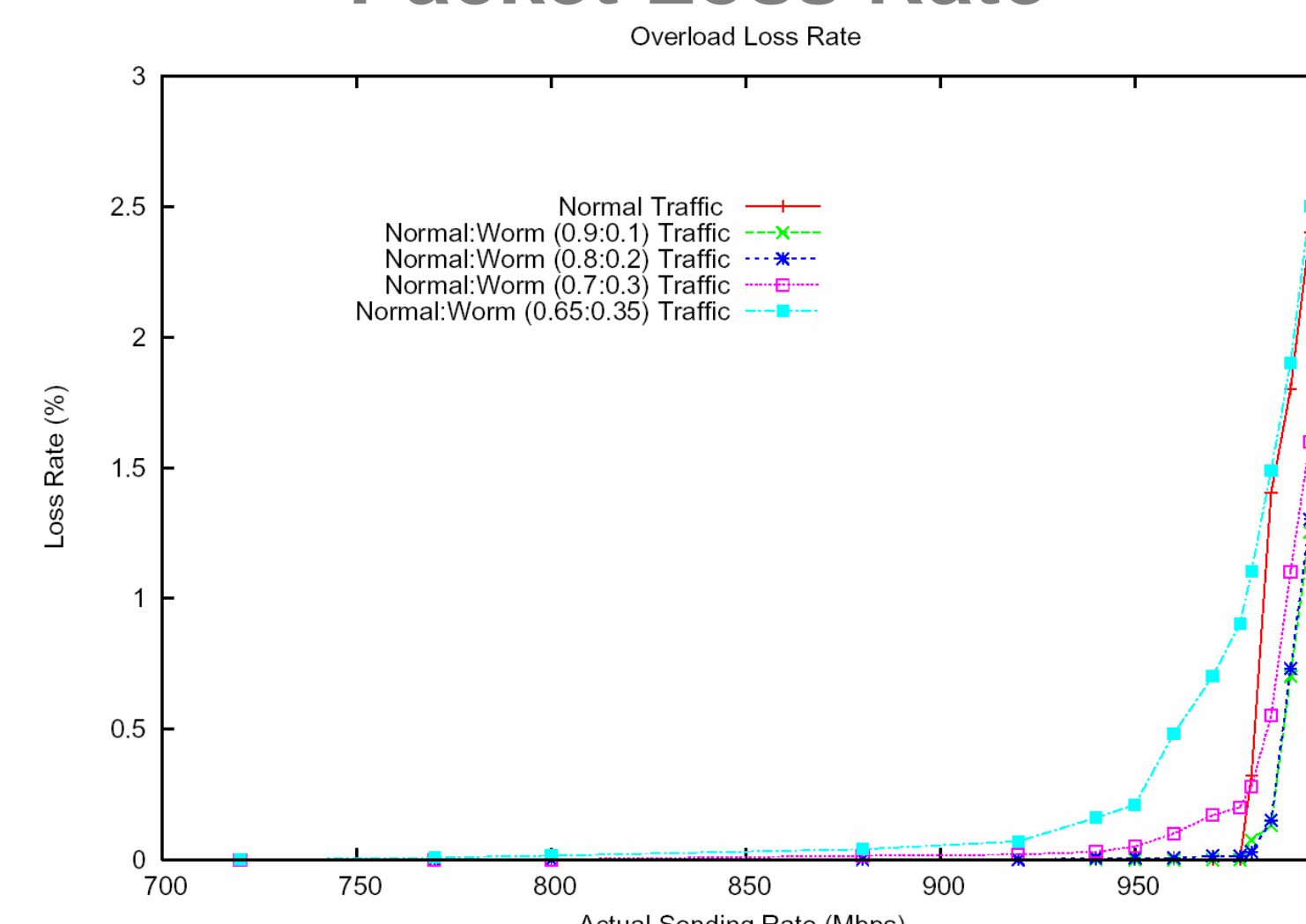


Gigabit Test-bed

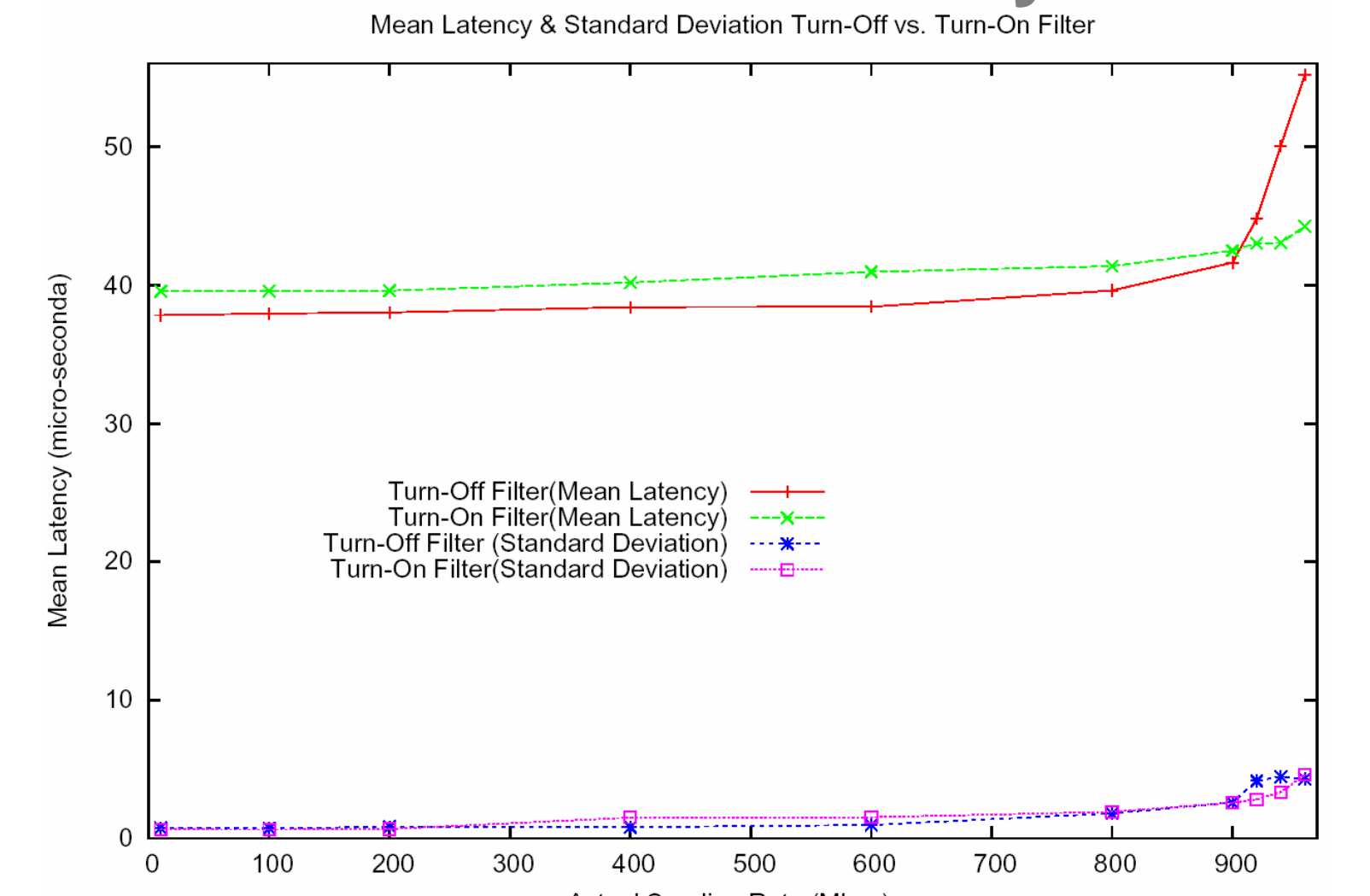


Evaluation

Packet Loss Rate



Packet Latency



Sponsors

